REMOTE ACCESS PROCEDURES

SSL-VPN TROUBLESHOOTING GUIDE

Date: 06/05/2009, Updated: 05/25/2012
Author: Bruce R. VanTassel

Contents:

Purpose....3
Operating Systems Support: 3
SSL-VPN Landing page download VPN client and establish a connection:....3
VPN Support....3
Common Errors and Solutions:....4
Message "Your device does not meet the requirements for logging on to the secure network … This client machine does not match the required security." 4
Message "The credentials you typed are incorrect. Please try again or contact your help desk or system administrator." 5
Message "Internet Explorer cannot display the webpage". 5
After establishing an SSL-VPN session, I can't seem to RDP to my workstation or reach any systems by system name.... 7
After establishing an SSL-VPN session, I can't seem to access the systems I need by name or IP address. 7
After establishing an SSL-VPN session, I can't seem to reach a certain system by name although other users can. I can reach the system by IP address and other systems by name. 8
I can't submit an SSL-VPN request or access the Internal Services links on http://connect.miamidade.gov/. My browser cannot find or display the page.... 8
Vendor/outside entity user is immediately logged off after establishing an SSL-VPN connection. 9
Computer crashes shortly after establishing an SSL-VPN session.... 9
Cannot connect; client log indicates: "*The Access Gateway Plugin received an invalid socket id*". 10
Message "The Network Configuration Lock is held by another application. Close all applications and run Setup again. ..." 10
Message "Checking System Configuration on your Device" when trying to connect. 11
Message "3006: The plugin failed to start. Contact your help desk or system administrator" 12

Message “Failed sending epaq” 12
Security Warning: “Do you want to view only the webpage content that was delivered securely?” 12
User not getting the static IP he was assigned. 13
Message “No IntranetIP available. Please try login later.” when trying to connect. 13
Message “The Correct Version of the NDIS Driver is not installed.” 13
Browser hangs at “Checking System Configuration on your Device” when attempting to connect. 14
Logon grayed out, (not accessible) on context menu of task bar icon. 15
SSL-VPN connection problems over AT&T wireless 3G using a County APN; mdc.org, mdcf.miamidade.gov, etc. 15
General Issues and Questions: 16
User cannot access local network resources when VPN is connected. 16
How to configure Access Gateway client split tunnel network options. 17
Cannot access http://connect.miamidade.gov/ on a miamidade.gov domain system that has its browser configured to use the County proxy server. 17
Can’t browse the internet after establishing a VPN connection 18
General troubleshooting steps 19

Purpose

This document was published to assist users, depot technicians and VPN staff when troubleshooting SSL-VPN issues. Common errors are listed along with detailed resolutions.

Operating Systems Support:

SSL-VPN connections are currently supported only for Windows XP 32 bit, Vista: 32 and 64 bit, Windows 7: 32 and 64 bit.

SSL-VPN Landing page download VPN client and establish a connection:

http://connect.miamidade.gov

VPN Support

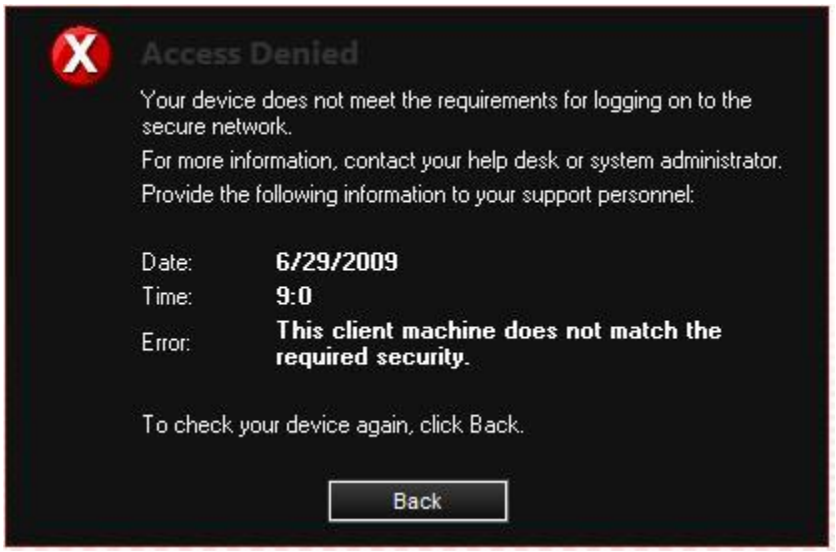
Tier 1 support is through Depot. Call 305-596-HELP and open up a help desk ticket.

Tier 2 support team is:

- Bruce VanTassel
- Robert Baril
- Keith Adams

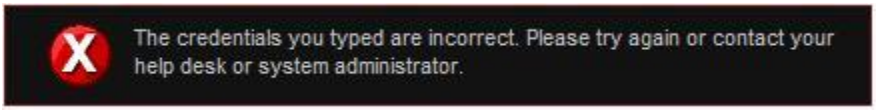
Common Errors and Solutions:

Message "Your device does not meet the requirements for logging on to the secure network … This client machine does not match the required security."



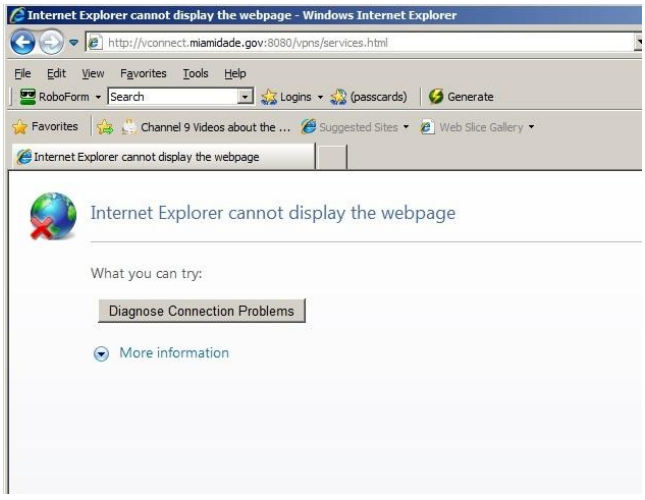
- Make sure you are running a supported anti-virus program, see: http://connect.miamidade.gov/faq.aspx.
- Make sure the Citrix Access Gateway Endpoint Analysis is installed. Internet Explorer initially blocks installation and running of Active-X controls. You may need to click a prompt to allow it to run.
- Make sure the Access Gateway Endpoint Analysis is allowed to run. Click Yes when prompted to run the scan.
- You need to be an administrator on the system to install the required plug-ins.

Message "The credentials you typed are incorrect. Please try again or contact your help desk or system administrator."



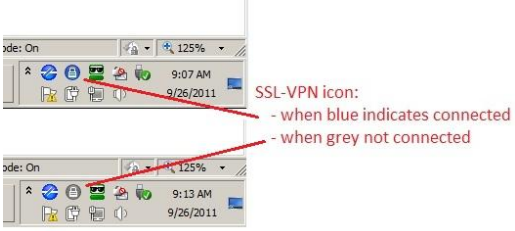
- If you have not done so, obtain authorization to use the SSL-VPN system; see: http://connect.miamidade.gov/demo.aspx, "How to request SSL-VPN access".
- You may have mis-keyed your user name or password; try again.
- Make sure you do not prepend the domain to your user name:
  - Correct: johnd
  - Incorrect: miamidade\johnd
- Make sure you are connecting to the correct SSL-VPN instance as listed on http://connect.miamidade.gov/, (try them both if you are not sure):
  - Employee or Full Time Consultant access: https://econnect.miamidade.gov
  - Vendor, Outside Entity, Expanded Employee access: https://vconnect.miamidade.gov
- Your account may be locked out due to too many failed login attempts. Wait 20 minutes for your account to automatically reset or contact the help desk to have it manually reset.
- There may be some other problem with your account; contact the help desk.

Message "Internet Explorer cannot display the webpage".



Make sure you don't have a firewall or proxy setting interfering with the traffic to the splash page.

Sometimes, the system is temperamental, especially when connecting from a slow or 3G wireless connection, and after logging in, the connected splash page does not show up. In many cases, the user is connected, (see screen dump below), but may not initially be able to reach any Metronet systems.



If connected and can reach the Metronet systems, there is no issue.

One problem frequently encountered is that some antivirus systems use a validation service that attempts to validate web pages before accessing. Trend does this with its web reputation service. When browsing, Trend will attempt to check the page through an Internet web service. If the client does not have Internet access after the initial VPN connection is established, the browser hangs for a period of time and typically times out. This is generally the case with County Domain systems that establish a non-split tunnel connection. To work around it, some users have been able to turn off the proxy, establish a connection, turn the proxy on. The connected splash page may not show up, but eventually a connection is established and Internet access possible through the County proxy.

If you cannot reach Metronet systems:

- Keep trying to connect to different systems for up to 5 minutes to see if the tunnel starts passing traffic.
- Reboot the client system and try again.
- You may have a split-tunnel conflict. For standard employee access try the non-split option, https://econnect2.miamidade.gov
- See also:
    - *After establishing an SSL-VPN session, I can't seem to RDP to my workstation or reach any systems by system name.*
    - *After establishing an SSL-VPN session, I can't seem to access the systems I need by name or IP address.*
    - *SSL-VPN connection problems over AT&T wireless 3G using a County APN; mdc.org, mdcf.miamidade.gov, etc.*

After establishing an SSL-VPN session, I can't seem to RDP to my workstation or reach any systems by system name.

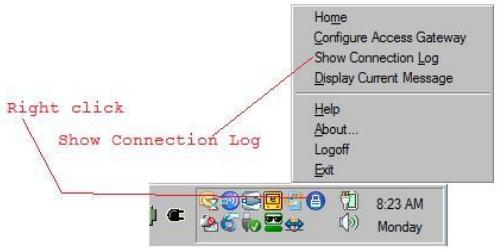
- Try appending the domain to the system name, ie. systemname.miamidade.gov.
- You may have a split-tunnel conflict. For standard employee access try the non-split option, https://econnect2.miamidade.gov.
- Make sure you don't have a firewall interfering with traffic to the system or support servers, (eg. DNS).
- See also *After establishing an SSL-VPN session, I can't seem to access the systems I need by name or IP address*.

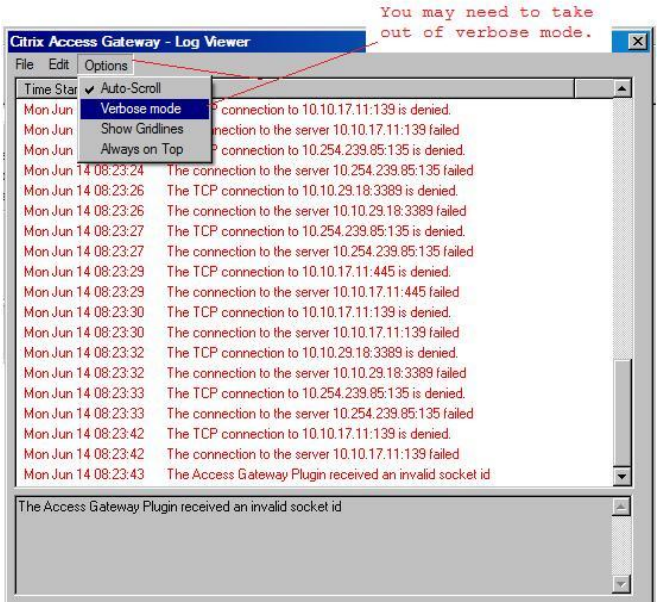
After establishing an SSL-VPN session, I can't seem to access the systems I need by name or IP address.

Insure that you have access to the systems you are trying to reach:

- If you have standard County employee access, see http://connect.miamidade.gov/ -> FAQ -> "Q: After connecting, what can I do?"
- You may have a special configuration. There is a Citrix bug that causes user configurations to not be applied when the alphabetic case of the account used to log in is different than what was configured on the device. Try logging in using lower case for your AD account:
  - Wrong: BRUCEVT
  - Correct: brucevt
- Make sure you do not prepend the domain to your user name:
  - Correct: johnd
  - Incorrect: miamidade\johnd
- Make sure you don't have a firewall interfering with traffic to the system or support servers, (eg. DNS).
- Also, check the connection log to see if access is being blocked, (see screen dump below). If so, you need to have a request for additional access submitted.

Continued next page …





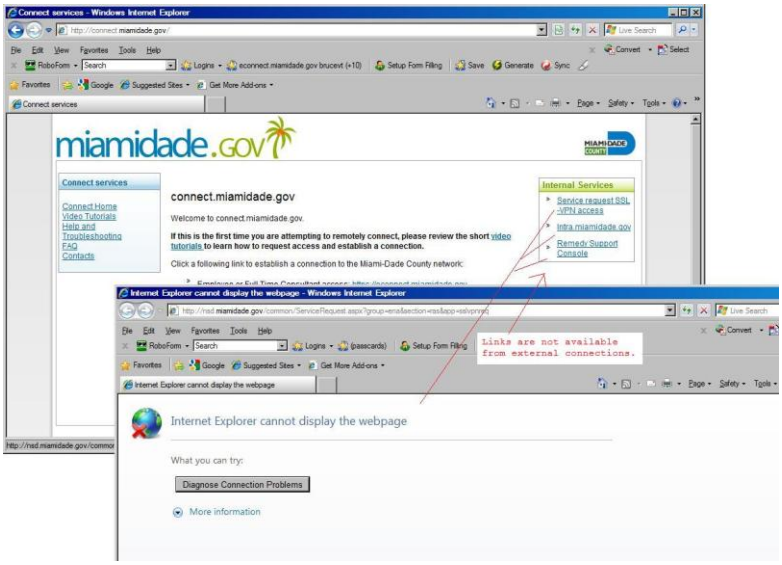
You may have a split-tunnel conflict. For standard employee access try the non-split option, https://econnect2.miamidade.gov.

After establishing an SSL-VPN session, I can't seem to reach a certain system by name although other users can. I can reach the system by IP address and other systems by name.

You've probably encountered yet another Citix bug; if the remote system name has the same name as a currently logged in user then the SSL-VPN device returns the IP address assigned to the SSL-VPN user, not the IP address of the system. If this is case, either access the system by IP address, change the name/DNS name of the system.

I can't submit an SSL-VPN request or access the Internal Services links on http://connect.miamidade.gov/. My browser cannot find or display the page.

Make sure you are attempting to use the internal services from within Metronet. These links are not available externally.



Vendor/outside entity user is immediately logged off after establishing an SSL-VPN connection.

The user's account has expired and needs renewed. Contact the County Employee responsible for the access to request extension from the Security Office.

There is a Citrix bug that causes user configurations to not be applied when the alphabetic case of the account used to log in is different than what was configured on the device.

- Try logging in using lower case for your AD account:
  - Wrong: BRUCEVT
  - Correct: brucevt
- Make sure you do not prepend the domain to your user name:
  - Correct: johnd
  - Incorrect: miamidade\johnd

Computer crashes shortly after establishing an SSL-VPN session.

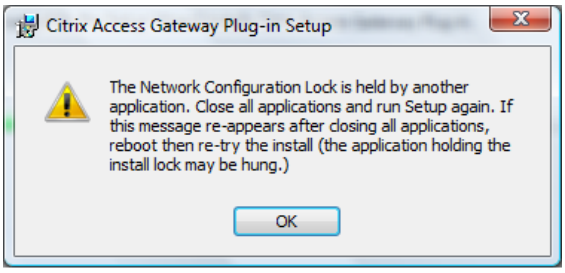
The Citrix Access Gateway client is incompatible with many other VPN clients. Completely uninstall all other VPN clients including other SSL-VPN clients, IPSEC clients, Netmotion, etc. Note that disabling the other clients may not be sufficient, they need to be completely removed from the system.

Note also that a problem has been identified with Vista and Windows 2008 clients, (STOP: 0x0000007F) that is resolved with a Microsoft hotfix. See http://support.microsoft.com/kb/972907 for information on issue and how to obtain and install the hotfix.

Cannot connect; client log indicates: "*The Access Gateway Plugin received an invalid socket id*".

The Citrix Access Gateway client is incompatible with many other VPN clients. Completely uninstall all other VPN clients including other SSL-VPN clients, IPSEC clients, Netmotion, etc. Note that disabling the other clients may not be sufficient, they need to be completely removed from the system.

Message "The Network Configuration Lock is held by another application. Close all applications and run Setup again. ..."



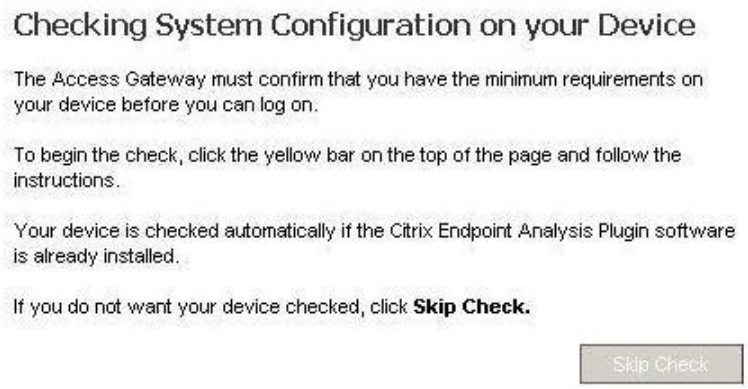
The Citrix Access Gateway client is incompatible with many other VPN clients. Completely uninstall all other VPN clients including other SSL-VPN clients, IPSEC clients, Netmotion, etc. Note that disabling the other clients may not be sufficient, they need to be completely removed from the system.

Message "Checking System Configuration on your Device" when trying to connect.

When establishing an initial connection, a page is displayed reading "Checking System Configuration on your Device" and nothing else happens.

Screen dump 1 example:

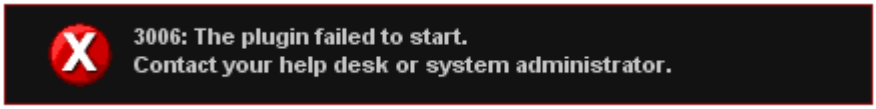
Screen dump 2 example:



There are a number of situations that can cause this problem:

- The user account using the client system is not an administrator on the machine. Make sure that an administrator logs into computer.
- A dialog is hidden behind the browser, (see below screen dumps in issue: *Browser hangs at "Checking System Configuration on your Device" when attempting to connect*).
- The client plug-in needs updated: click download and follow the process to upgrade the client, (see http://connect.miamidade.gov/ -> Click "Video Tutorials" -> Click "*What happens when a new plug-in version is released*").

Message "3006: The plugin failed to start. Contact your help desk or system administrator"



Make sure you are running Internet Explorer 6 or above.

Message "Failed sending epaq"

A wonderfully intuitive Citrix error message. Solutions:

- Make sure you are running Internet Explorer 6 or above.
- Check to see if anything may be blocking traffic, (eg. a local or network firewall, etc).

Security Warning: "Do you want to view only the webpage content that was delivered securely?"

This is a counter intuitive, Citrix and Microsoft bug that occurs with some browser versions. Click No to continue.

You can disable this warning by:

1. Going to Tools->Internet Options->Security
2. Select the 'Security' tab
3. Click the 'Custom Level' button
4. In the 'Miscellaneous' section change "Display mixed content" to Enable

User not getting the static IP he was assigned.

There is a Citrix bug that causes user configurations to not be applied when the alphabetic case of the account used to log in is different than what was configured on the device. Try logging in using lower case for your AD account:

- Wrong: BRUCEVT
- Correct: brucevt

Message "No IntranetIP available. Please try login later." when trying to connect.

There is a Citrix bug that causes this message when the alphabetic case of the account used to log in is different than what was configured on the device. Try logging in using lower case for your AD account:

- Wrong: BRUCEVT
- Correct: brucevt

Message "The Correct Version of the NDIS Driver is not installed."

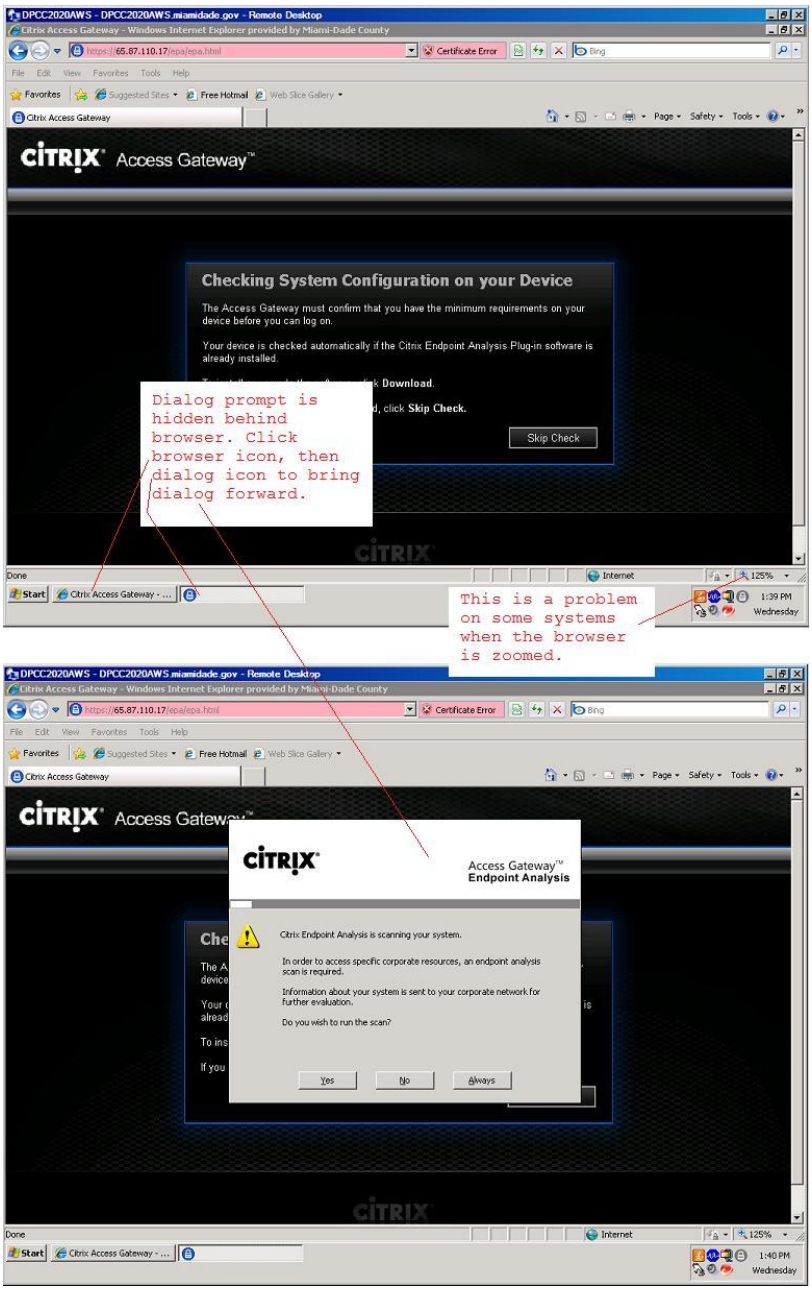
Another Citrix bug; solution:

- Uninstall the Citrix Access Gateway Plug-in, (using Control Panel -> Add or Remove Program, or Control Panel -> Programs and Features)
- Reboot
- Go through the process of establishing an SSL-VPN connection and reinstalling the plug-in.

Document continued on next page.

Browser hangs at "Checking System Configuration on your Device" when attempting to connect.

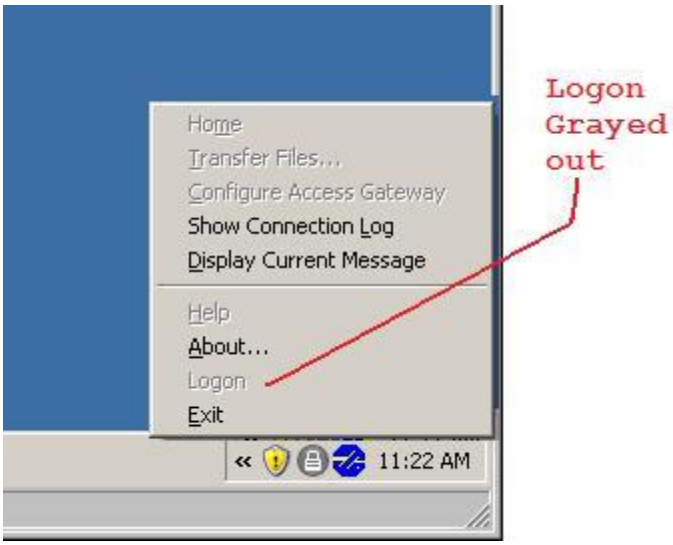
On some systems, the browser can seem to hang at "Checking System Configuration on your Device". The problem is that a dialog prompt is masked by the browser, (see screen dump below). This typically happens of the browser is zoomed.



Logon grayed out, (not accessible) on context menu of task bar icon.

If "Logon" is not accessible on context menu of task bar icon, (see screen dump below), the URL configuration of the connection has somehow been lost. To connect, simply go to the SSL-VPN min-portal, (http://connect.miamidade.gov) and click the appropriate link to re-establish the URL configuration and connect:

- Employee or Full Time Consultant access: https://econnect.miamidade.gov
- - or -
- Vendor, Outside Entity, Expanded Employee access: https://vconnect.miamidade.gov)



SSL-VPN connection problems over AT&T wireless 3G using a County APN; mdc.org, mdcf.miamidade.gov, etc.

SSL-VPN access can be a pain over AT&T wireless 3G. Try the following, make sure you have a solid connection, connect with split-tunneling turned off - go to http://connect.miamidade.gov/ and click No split tunnel: https://econnect2.miamidade.gov. You may have to turn your proxy settings off. After connecting, turn County proxy settings on to get to the Internet.

With the SSL-VPN over 3G; one problem frequently encountered is that some antivirus systems use a validation service that attempts to validate web pages before accessing. Trend does this with its web

reputation service. When browsing, Trend will attempt to check the page through an Internet web service. Since the client does not have Internet access, the browser hangs for a period of time and typically times out. To work around it, some users have been able to turn off the proxy, establish a connection, turn the proxy on. Typically the connected splash page does not show up, but eventually a connection is established.

Netmotion is the supported environment for mobile access. It is designed to handle these and other situations that arise when attempting remote connections over unstable wireless connections.

See also section *Message "Internet Explorer cannot display the webpage"*.

General Issues and Questions:

User cannot access local network resources when VPN is connected.

Access to local network resources while having an SSL-VPN connection is configured by remote access administrative staff by a setting called split tunneling. Due to security restrictions, split tunneling is only allowed for County employees using non-County systems that have VPN access restricted to rdp, http and https traffic, (most employee accounts are configured to be restricted). Accounts that have less restrictive access and non-County users are not configured with split tunneling.

Split tunneling routes all 10.0.0.0/8 IP addresses and the County owned external IP address space, 65.87.64.0/18 to the tunnel. If these IP addresses conflict with the local network then access to local resources having conflicting IP addresses will not be possible.

If split tunneling is not permitted or if there is an IP address space conflict, an unsupported work-around is to install virtual PC on the client system, configure a virtual machine, install XP on the virtual machine and established the VPN connection through the virtual machine. In this way the host client system can access the local network and the virtual machine can access the County network through VPN.

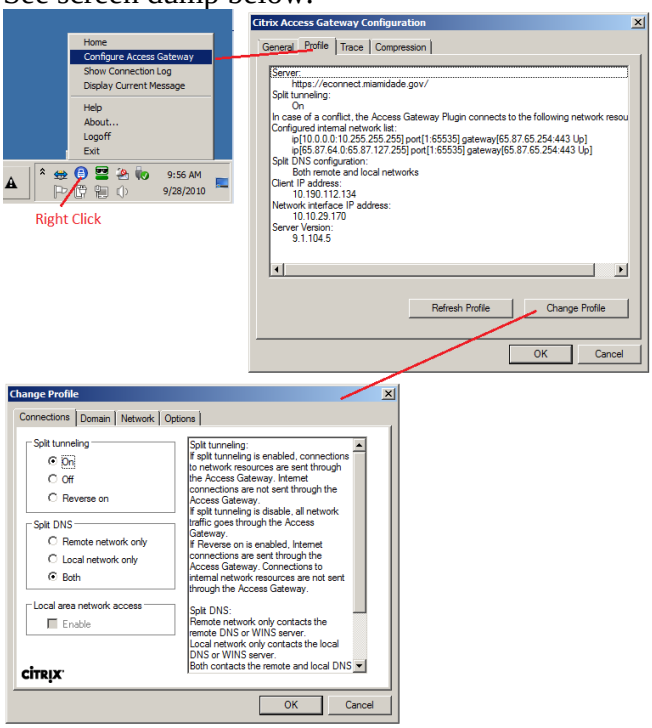
See also *How to configure Access Gateway client split tunnel network options* below.

How to configure Access Gateway client split tunnel network options.

County employees: the easiest way to establish a non-split tunnel option is to go to http://connect.miamidade.gov/ and select the non-split option, https://econnect2.miamidade.gov.

If your connection is permitted split tunneling, it can be toggled off and on and certain options can be set at the client after the connection is established: right click the AG icon -> Configure Access Gateway -> Change Profile: change various settings in the Connections, Domain and Network tabs.

See screen dump below.



Cannot access http://connect.miamidade.gov/ on a miamidade.gov domain system that has its browser configured to use the County proxy server.

There is a problem with pre-IE8 browsers when configured with proxy access. Make sure you are running Internet Explorer 8 or above. Also,

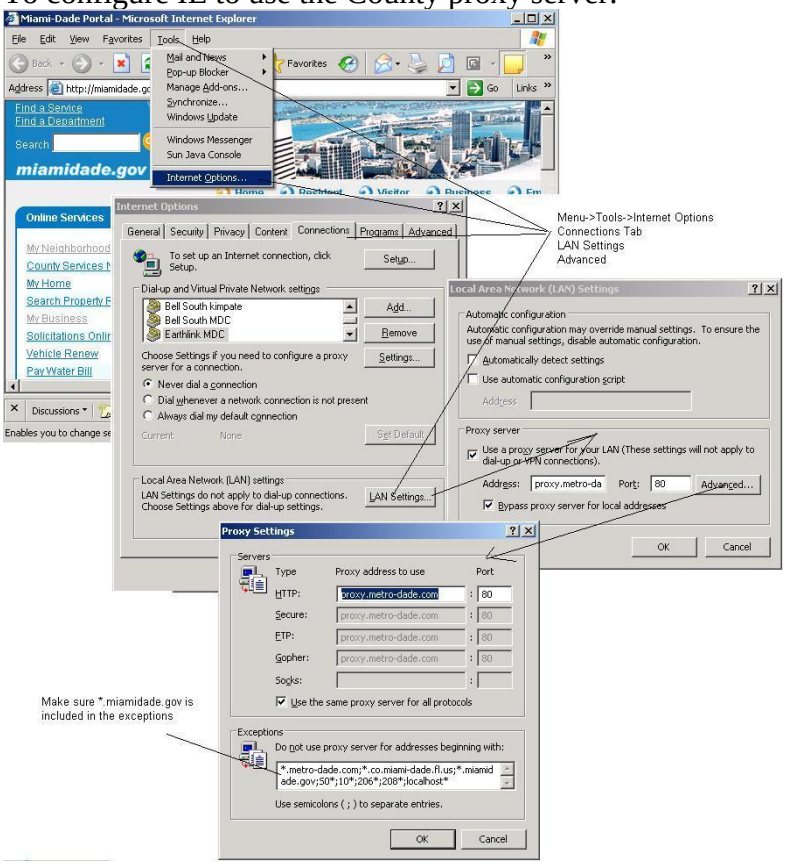
insure that an appropriate proxy exception, (*Do not user proxy server for addresses beginning with:*) is configured, (ie. *.miamidade.gov).

See the section "Can't browse the internet after establishing a VPN connection", (below) for a description/screen dump of how to configure proxy settings.

Can't browse the internet after establishing a VPN connection

For non-split tunneled connections, internal sites, (miamidade.gov, intra.miamidade.gov, etc.) can be accessed with or without a proxy configuration. To get out to the internet, you need to configure to use the proxy, (Proxy.miamidade.gov). The simplest thing to do is to have the user remote to their workstation and run IE from there.

To configure IE to use the County proxy server:



Split tunneled connections should not encounter this problem.

General troubleshooting steps

In addition to the information given elsewhere in this document, the following describes general VPN troubleshooting steps:

- First insure that the system has internet access.
- Insure that Internet Explorer 6 or above is used to establish the SSL-VPN connection.
- Validate you are using a supported operating system: see http://connect.miamidade.gov/faq.aspx
- Validate the connect user is an administrator on the system.
- Reboot the computer and see if that resolves the problem.
- Narrow the source of the problem: The issue may be either with the system, remote router, user account or the DSL line. Actions to narrow the problem: reboot the computer; try logging on to VPN with different domain account; bypass the router and connect directly to the DSL modem; connect the computer to a known working connection; connect a known working computer to the DLS modem/router.
- If the problem is with the computer, some things to try:
    1. Disable firewall software.
    2. Uninstall and reinstall the VPN software.
    3. Change the network interface card with a different vendor/model.
    4. Log on as a different local account to see if there may be a profile issue.
    5. Look for software that may be interfering with the connection. Anything that might access the network or internet is suspect. We've experience issues with instant messenger software, other VPN software, wireless card drivers, etc.
    6. Reinstall the operating system.
- If the problem is with the router:
    1. Check to see if a firmware update is available.
    2. Look to see if there is anything blocking UDP port 500 traffic.
    3. Replace the router.
- If the problem is with the user account:
    1. Insure the account is not disabled, not locked out, has an expired password, etc.
    2. Make sure that account the password is not expired or that the account is not set to force user to change password at next logon.
    3. Check to see that the account is a member of a group allowed VPN access.
    4. The Dial-in tab that remote access is allowed and no callback is selected.
- If the problem is with the DSL line, (highly unlikely, but possible):
    1. Contact the DSL vendor